Instruction

Acceptable Use Policy for Employees Using District Technology

Purpose:
The Peoria Public Schools District 150 Technology Network is made available to all staff and students to support the educational goals and mission of the District. Access to the local network, including Internet resources, is given to aid in research, enhance productivity, upgrade skills, educate students and to foster the exchange and collaboration of information with peers and the local community.

Network use:

- Only users with authorized access can use standalone or networked computers; District authorized wireless devices; and their resources. Logging into a computer or the network using someone else's login is prohibited.
- Any user identified as a security risk may be denied access to the network.
- Network resources will not be used for commercial business nor political or religious purposes
- Any use of the network for illegal activity is prohibited.
- Use of the system to access material that is considered pornographic in nature, or that advocates violence, illegal activities, or discrimination toward other people is prohibited.
- Sending material likely to be offensive or objectionable to others is prohibited.
- Restrictions are placed on access to some programs and computer resources in order to maintain network security, and ensure that the equipment is available and functional for all users.
- Access to some applications and Internet resources has been restricted by blocking software. Unauthorized use of equipment, attempting to access intentionally blocked software or making modifications to equipment/software by any means, is prohibited.
- Access to Internet streaming media is prohibited except for educational purposes. Streaming media includes but is not limited to; Internet radio, television, YouTube, Google Video, etc.
- Users will notify the system administrator if a security problem is identified.

Account Security

- Any user who has been assigned a network account is responsible for its security and should take all reasonable precautions to prevent others from being able to use it.
- Under no condition will you provide your password or account information to another person.
- If required, you will regularly change your passwords using a combination of letters and numbers.
- You will not share your account with anyone nor leave the account open or unattended.
- You will notify the District or Technology immediately if you suspect your account has been accessed illegally.

Software/Data

- The illegal installation of copyrighted software or files onto District computers is prohibited.
- Installation of any software on District computers must be coordinated with the District Technology office.

- You will not improperly access, misappropriate, or misuse the files, data, or information of others.
- You are responsible to take precautions to prevent the proliferation of viruses between your personal equipment, Peoria Public Schools District 150 equipment, and any other equipment accessed via the District network.
- Although the District schedules back-ups of District servers nightly, you are responsible for making back-up copies of the documents that are critical to you.

Hardware

- You will not improperly access, misappropriate, misuse, or abuse District communications or technology equipment.
- You will not add, remove, or re-locate any equipment (e.g. computers, printers, network cards, cables, etc) from any District network location without prior coordination with the District Technology office.
- Any equipment assigned to you becomes your responsibility. Use of that equipment on or off campus, that is considered inappropriate by the definitions outlined in the document, becomes a violation of this agreement and is cause for disciplinary action.

Search and Seizure

- You should expect only limited privacy in the contents of your records of your on-line activity.
- Routine maintenance and monitoring of the Network may lead to discovery that you have violated this Policy or the law.
- Use of the network may be subject to Family Educational Rights and Privacy Act (FERPA), Freedom of Information Act (FOIA), Illinois Student Records Act (ISRA), and discovery in civil litigation.
- Records related to network usage may be produced for the public that requests documents pursuant to FOIA, opposing parties in litigation with a district, parents and students requesting information under ISRA, FOIA, and FERPA.
- An individual search will be conducted if there is reasonable suspicion that you have violated this Policy or the law.
- If the law is violated by the use of District technology equipment or network, legal authorities may institute a search and seizure process.

Email

Email is provided to the Peoria Public Schools District 150 staff to be used primarily for internal and external business communications. All GroupWise email accounts are owned by Peoria Public Schools District 150. District email accounts are not private.

The District retains the right to review, audit, intercept, access and disclose all messages created, received, or sent on the electronic mail system as necessary. District provided email is not private or protected. Remote access to email accounts is available over the Internet; all policies apply to out-of-network access.

Personal use of the District email is strongly discouraged.. Email usage should not interfere with the day to day duties of staff, nor should it violate either the Board of Education's policies or the following points:

- Staff use of email should not promote, or support political functions or agendas in any way, both internally and externally, unless approved by the Superintendent.
- Staff use of email should not promote, or support private business or industry, especially the originators own private concern or business.
- Staff use of email should not promote illegal activities or activities prohibited by district policy as found in this document of Board of Education policies.
- Staff shall not engage in internal or external email activities that are regarded as spam or mass emailing unless for information purposes that are approved by District administration.
- Staff shall not create or forward "chain letters" or other "pyramid" schemes of any type via email.

Spam is defined as email that is sent to multiple individuals in an uninvited manner for purposed of furthering a private and/or political agenda, the transmission of questionable material, or as a means of solicitation.

Expectation of Privacy

You should expect no privacy in the contents of any files on the District system. Peoria Public Schools District 150 owns and operates all hardware, software, and data on the network. The District will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities not in compliance with District policies conducted through the District network.

- Routine maintenance and monitoring of the District network may lead to a discovery that a user has violated this policy, another District policy, or the law.
- All District email is subject to release to the public under the Illinois Freedom of Information Act.
- An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or District policy.
- Parents have the right at any time to investigate or review the contents of their students' files.
- Parents have the right to request the termination of their child's individual access to the network at any time.

Limitation of Liability

- The District makes no guarantee that the functions or services provided by or through the District network will be error-free or without defect.
- The District is not responsible for any damage the user may suffer, including but not limited to, loss of data or interruptions of service.
- The District is not responsible for the accuracy or quality of the information obtained through, or stored on the network.
- The District will not be responsible for financial obligations resulting from the unauthorized use of the network.

District Staff Responsibilities

- Never post any personal contact information about yourself or others. This includes your social security number, address, phone, credit cards, school/work address, etc.
- Staff must monitor lists of students who either do not have permission to use the network resources or who have had those privileges revoked to ensure that those students are not gaining access to those resources.
- Teachers are responsible for monitoring student use of District technology at all times.

- Any student who does not have permission to use the network resources or who has had those privileges revoked must be provided with an alternative means of meeting the class objectives.
- Users will follow all copyright laws. Copyright infringement is the sole responsibility of the person violating the copyright law and that the District shall be held harmless. All liability for such action will rest with the individual.
- All users will sign annually the Acceptable Use Policy to be maintained as part of the staff member's record.

Confidentiality

All users of the District's computers/network (both on the network and/or on the Internet in a location out of a District building) shall maintain the confidentiality of student records as required by law. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded on to the network.

- Teachers are to secure computer screens while using Gradebook online and any other technology tool that addresses student information such as Skyward.
- Teachers are not to discuss a student identified by name in any electronic communication.
- Discipline records of students are confidential.

Penalties

- Any user violating these provisions, applicable state and federal laws, or posted classroom and district rules is subject to loss of network privileges and any other district disciplinary options.
- School and district administration will make the final determination as to what constitutes unacceptable use.

Legal Ref: Illinois Freedom of Information Act. 5 ILCS 140/1 et seq.
Illinois Student Records Act. 105 ILCS 10/1 et seq.

Adopted: June 1, 2009